

AMENDMENTS TO THE CLAIMS

Claim 1. (Previously presented) An illegal access data handling apparatus, comprising:

a control system; and

a decoy server, functionally coupled to the control system, wherein the apparatus is placed outside a given internal communication network, for receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network, and for taking countermeasures against the illegal access data received, further wherein the countermeasures include providing a response pretending to originate from the internal communication network,

the response being encapsulated and sent to a network device within said given internal communication network to be decapsulated and transmitted by the network device to said data communication device.

Claim 2. (Previously Presented) The illegal access data handling apparatus of claim 1, wherein the illegal access data handling apparatus is connected to an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network, and for detecting the illegal access data, and

wherein the illegal access data handling apparatus receives the illegal access data from the illegal access data detection device.

Claim 3. (Previously Presented) The illegal access data handling apparatus of claim 2, further comprising:

a data reception section for receiving the illegal access data from the illegal access data detection device;

a data analysis section for analyzing the illegal access data received by the data reception section;

a response data generation section for generating response data to the illegal access data based upon an analysis result from the data analysis section; and

a data transmission section for transmitting the response data generated by the response data generation section to the illegal access data detection device.

Claim 4. (Previously Presented) The illegal access data handling apparatus of claim 3, wherein the data reception section receives an encapsulated illegal access data from the illegal access data detection device,

wherein the illegal access data handling apparatus further includes a encapsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data, and
wherein the data transmission section transmits the response data encapsulated by the encapsulation section to the illegal access data detection device.

Claim 5. (Original) The illegal access data handling apparatus of claim 3, wherein the response data generation section generates response data having same contents as those of response data that would be generated by a specific data communication device placed in the internal communication network in response to the illegal access data if the specific data communication device received the illegal access data.

Claim 6. (Original) The illegal access data handling apparatus of claim 3, wherein the data reception section receives from the illegal access data detection device communication history information indicating a communication history of the illegal access data detection device,

wherein the data analysis section analyzes the communication history information received by the data reception section, and generates illegal access data designation information designating data transmitted from a given data communication device placed outside the internal communication network as the illegal access data based upon an analysis result of the communication history information, and

wherein the data transmission section transmits the illegal access data designation information generated by the data analysis section to the illegal data detection device.

Claim 7. (Original) The illegal access data handling apparatus of claim 4, wherein the data reception section receives the illegal access data having authentication information attached to be used for data authentication from the illegal access data detection device, and

wherein the encapsulation section performs the data authentication for the illegal access data by using the authentication information.

Claim 8. (Original) The illegal access data handling apparatus of claim 7, wherein the encapsulation section attaches the authentication information to be used for the data authentication for the response data to the response data, and

wherein the data transmission section transmits the response data having the authentication information attached by the encapsulation section to the illegal access data detection device.

Claim 9. (Previously presented) A method for handling illegal access data outside a given internal communication network, the method comprising:

receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network; and

taking countermeasures against the illegal access data received by a data center remotely located over the Internet from the internal network, wherein the countermeasures include providing a response pretending to originate from the internal communication network,

the response being encapsulated by the data center and sent to a network device within said internal communication network to be decapsulated and transmitted by the network device to said data communication device.

Claim 10. (Previously Presented) The method of claim 9, comprising:

communicating with an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network, and for detecting the illegal access data; and

receiving the illegal access data from the illegal access data detection device.

Claim 11. (Original) The method of claim 10, comprising:

receiving the illegal access data from the illegal access data detection device;

analyzing the illegal access data received by the receiving;
generating response data to the illegal access data based upon an analysis result from the analyzing; and

transmitting the response data generated by the generating to the illegal access data detection device.

Claim 12. (Original) The method of claim 10, generates response data having same contents as those of response data that would be generated by a specific data communication device placed in the internal communication network in response to the illegal access data if the specific data communication device received the illegal access data.

Claim 13. (Currently amended) A method for responding to unauthorized access packet to an internal communications network, comprising:

receiving an encapsulated unauthorized access packet at a data center placed outside the internal network, and wherein the unauthorized access packet is redirected from a target server residing within the internal network;

analyzing the received packet to formulate a response packet;

encapsulating the response packet so that it appears to originate from the target server; and

sending the encapsulated response packet to a network device, wherein the network device is within the internal network, and wherein the network device decapsulates the encapsulated response packet and forwards the decapsulated packet to the source of the unauthorized access packet.

Claim 14. (Previously Presented) The method according to claim 13, further comprising:

determining if the encapsulated unauthorized access packet was transmitted from a client;

judging whether data of the encapsulated unauthorized access packet came from an unauthorized source;

analyzing the encapsulated unauthorized access packet based upon data from a knowledge base; and

notifying a decoy server of the analysis result.

Claim 15. (Previously Presented) The method according to claim 14, further comprising:

referring to a client database; and

collating the encapsulated unauthorized access packet with information contained in the client database.

Claim 16. (Previously Presented) The method according to claim 14, further comprising:

accessing a knowledge base having information associated with past encapsulated unauthorized access packets.

Claim 17. (Cancelled).